UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,862	02/25/2004	Sergey Shokhor	08204/0200873-US0	3678

38878 7590 03/26/2008

F5 Networks, Inc.
c/o DARBY & DARBY P.C.
P.O. BOX 770
Church Street Station
NEW YORK, NY 10008-0770

EXAMINER	
KEEHN, RICHARD G	

ART UNIT	PAPER NUMBER
2152	

MAIL DATE	DELIVERY MODE
03/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/786,862	SHOKHOR ET AL.	
	Examiner	Art Unit	
	Richard G. Keehn	2152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-34 have been examined and are pending.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 28-30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. A signal is not a process, machine, manufacture or composition of matter, hence a signal is non-statutory.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-2, 4-5, 7, 10-11, 13-16, 21-23, 25, 28 and 30-31 are rejected under 35 U.S.C. 102(b) as being anticipated by US 6,954,792 B2 (Kang et al.).

As to Claim 1, Kang et al. anticipate an apparatus for managing access to a resource over a network, comprising:

a receiver arranged to receive a request for access to the resource from a client device (Kang et al. – Figure 4, item 400, as well as Column 13, line 1 recite the client sending a connection request for access to resources to a server); and

a policy manager (Kang et al. – Figure 4, item 412, as well as Column 13, lines 20-29 recite the authentication protocol handler), coupled to the receiver, that is arranged to perform actions, including:

determining a configuration of the client device (Kang et al. - Figure 4, item 402, as well as Column 13, lines 2-3 recite the determination of authentication type for the requesting client); and

applying a dynamic policy for the access based, in part, on the determined configuration (Kang et al. – Column 13, lines 3-5 recite the client and server negotiating the authentication type, when is a dynamic process); and

applying a restriction to the access for the requested resource based on the applied dynamic policy (Kang et al. – Figure 4, item 416 recites the denial of client access to server resources).

As to Claim 2, Kang et al. anticipate the apparatus of claim 1, wherein determining the configuration of the client device further comprises:

if the client device is configured to receive a downloadable component, providing the downloadable component to the client device (Kang et al. – Figure 5, items 506 and 510 recite determining if the client is authorized to receive resources, and providing access to the resources once authorized.).

As to Claim 4, Kang et al. anticipate the apparatus of claim 1, wherein determining the configuration of the client device further comprises determining information associated with the connection between the client device and the resource (Kang et al. – Figure 4, item 402 recites the determining of the authentication, which is associated with connection).

As to Claim 5, Kang et al. anticipate the apparatus of claim 1, further comprising in response to receiving the request for access to the resource, transmitting a downloadable component to the client device (Kang et al. – Figure 5, items 500, 506 and 510 recite allowing the client to download the resource in response to a request for the resource and after authentication).

As to Claim 7, Kang et al. anticipate the apparatus of claim 1, wherein the restriction includes at least one downloadable component (Kang et al. – Figure 5, item 510 recites the client gaining access to the server resources, which are downloaded from server to client).

As to Claim 10, Kang et al. anticipate a method of managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device (Kang et al. – Figure 4, item 400 recites the client sending a connection request for access to resources to a server).

determining a configuration of the client device (Kang et al. - Figure 4, item 402 recites the determination of authentication type for the requesting client);

applying a dynamic policy for the access based in part, on the determined configuration (Kang et al. – Column 13, lines 3-5 recite the client and server negotiating the authentication type, when is a dynamic process); and

applying a restriction to the access for the requested resource based on the applied dynamic policy (Kang et al. – Figure 4, item 416 recites the denial of client access to server resources).

As to Claim 11, Kang et al. anticipate the method of claim 10, further comprising in response to receiving the request for access to the resource, transmitting a downloadable component to the client device (Kang et al. – Figure 5, items 500, 506 and 510 recite allowing the client to download the resource in response to a request for the resource and after authentication).

As to Claim 13, Kang et al. anticipate the method of claim 10, wherein determining the configuration further comprises determining at least one of one level of trust associated with the client device, a type of encryption enabled on the client device, a type of antivirus enabled on the client device, a security feature enabled on the client

device, a browser type, an operating system configuration, a security certificate, and if a hacker tool is enabled on the client device (Kang et al. – Figure 4, item 414 recites determining client authentication which is a level of trust).

As to Claim 14, Kang et al. anticipate the method of claim 10, wherein determining the configuration further comprises determining a level of trust of the client device (Kang et al. – Figure 4, item 414 recites determining client authentication which is a level of trust).

As to Claim 15, Kang et al. anticipate the method of claim 10, wherein determining the configuration further comprises determining a characteristic of an enabled security application enabled (Kang et al. – Figure 4, item 414 recites the determination of authenticity, which is a security application).

As to Claim 16, Kang et al. anticipate the method of claim 10, wherein applying the restriction further comprises downloading a component to the client device (Kang et al. – Figure 5, items 506, 508 and 510 recite the granting or not granting of access to the client).

As to Claim 21, Kang et al. anticipate the method of claim 10, wherein applying the dynamic policy further comprises restricting the access to the resource (Kang et al.

– Figure 5, item 508 recites restricting access to the client based on the authentication policy).

As to Claim 22, Kang et al. anticipate a network appliance for managing access to a resource over a network, comprising:

a transceiver for receiving a request for access to the resource from a client device (Kang et al. – Figure 4, item 400 recites the client sending a connection request for access to resources to a server); and

a processor that is configured to perform actions, including:

receiving the request for access (Kang et al. – Figure 4, item 400 recites the client sending a connection request for access to resources to a server);

determining a configuration of the client device (Kang et al. - Figure 4, item 402 recites the determination of authentication type for the requesting client).

applying a dynamic policy for the access based in part, on the determined configuration (Kang et al. – Column 13, lines 3-5 recite the client and server negotiating the authentication type, when is a dynamic process).

applying a restriction to the access for the requested resource, wherein the restriction is configured based on the applied dynamic policy (Kang et al. – Figure 4, item 416 recites the denial of client access to server resources).

As to Claim 23, Kang et al. anticipate the network appliance of claim 22, wherein the processor is configured to perform further actions, comprising:

in response to receiving the request for access to the resource, transmitting a downloadable component to the client device (Kang et al. – Figure 5, items 500, 506 and 510 recite allowing the client to download the resource in response to a request for the resource and after authentication).

As to Claim 25, Kang et al. anticipate the network appliance of claim 23, wherein determining the configuration of the client device further comprises:

if the client device is configured to receive a downloadable component, providing the downloadable component to the client device (Kang et al. – Figure 5, item 504 recites determining if the client is authorized to receive resources, and providing access to the resources once authorized).

As to Claim 28, Kang et al. anticipate a modulated data signal for managing access to a resource over a network, the modulated data signal comprising the actions of:

receiving a request for access to the resource from a client device (Kang et al. – Figure 4, item 400 recites the client sending a connection request for access to resources to a server).

sending a configuration of the client device (Kang et al. – Figure 4, items 400 and 402 recite the client sending a connection request for access to resources to a server including its authentication type);

applying a dynamic policy to the access based in part, on the sent configuration (Kang et al. – Column 13, lines 3-5 recite the client and server negotiating the authentication type, when is a dynamic process).

applying a restriction to the access for the requested resource based on the applied dynamic policy (Kang et al. – Figure 4, item 416 recites the denial of client access to server resources).

As to Claim 30, Kang et al. anticipate the modulated data signal of claim 28, wherein applying the restriction further comprises blocking a download of at least one file to the client device (Kang et al. – Figure 5, item 508 recites blocking client access to information on the server).

As to Claim 31, Kang et al. anticipate an apparatus for managing access to a resource over a network, comprising:

a transceiver arranged to receive a request for access to the resource from a client device (Kang et al. – Figure 4, item 400 recites the client sending a connection request for access to resources to a server); and

a policy manager (Kang et al. – Figure 4, item 412 recites the authentication protocol handler), coupled to the transceiver, that is arranged to perform actions, including:

a means for determining a configuration of the client device (Kang et al. - Figure 4, item 402 recites the determination of authentication type for the requesting client); and

a means for applying a dynamic policy for the access based, in part, on the determined configuration (Kang et al. – Column 13, lines 3-5 recite the client and server negotiating the authentication type, when is a dynamic process).; and

a means for restricting to the access for the requested resource, wherein the means for restricting is configured based, in part, on the applied dynamic policy (Kang et al. – Figure 4, item 416 recites the denial of client access to server resources).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kang et al. as applied to claim 1, and further in view of Non-Patent Literature on the Print Distributor 2.0 system (Print Distributor 2.0).

As to Claim 8, Kang et al. disclose an invention substantially as claimed, including the apparatus of claim 1.

Kang et al. do not disclose, but Print Distributor 2.0 disclose an invention substantially as claimed, including wherein the restriction is configured to intercept a communication between the client device and the apparatus (Print Distributor 2.0 – Pages 1-3 recite the downloadable resource called Print Distributor 2.0 which intercepts print files and restricts the launching of the print job to the printer by allowing redirection to a file).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine applying a restriction to the access for the requested resource based on the applied dynamic policy taught by Print Distributor 2.0, with a receiver arranged to receive a request for access to the resource from a client device and a policy manager, coupled to the receiver, that is arranged to perform actions taught by Kang et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to provide a means to execute the security access policy by interception and restriction (Print Distributor 2.0 - pages 1-3).

As to Claim 9, Kang et al. disclose an invention substantially as claimed, including the apparatus of claim 1.

Kang et al. do not disclose, but Print Distributor 2.0 discloses an invention substantially as claimed, including wherein applying the restriction further comprises performing at least one of intercepting a system command, inhibiting a file save, inhibiting a file print, restricting launching of a predetermined application, and redirecting access to a file (Print Distributor 2.0 – Pages 1-3 recite the downloadable resource called Print Distributor 2.0 which intercepts print files and restricts the launching of the print job to the printer by allowing redirection to a file).

The motivation and obviousness arguments are the same as in Claim 8.

5. Claims 3 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kang et al. as applied to claims 2 above, and further in view of US 6,502,131 B1 (Vaid et al.).

As to Claim 3, Kang et al. anticipate the apparatus of claim 2.

Kang et al. do not disclose, but Vaid et al. disclose an invention substantially as claimed, including wherein the downloadable component is configured to inspect an environment of the client device and provide environment information to the policy manager (Vaid et al. – Column 23, lines 38-59 recite the active probing of devices on the network and providing statistics to management components, one of which being the Enterprise Policy Manager).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine inspect an environment of the client device and provide environment information to the policy manager taught by Vaid et al., with providing the downloadable component to the client device taught by Kang et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to allow a means to analyze policies of devices on the network to assist in traffic and enforcement (Vaid et al – Column 23, lines 38-46).

As to Claim 12, Kang et al. anticipate the method of claim 10, wherein determining the configuration further comprises, if the client device is configured to receive a downloadable component, providing the downloadable component to the

client device (Kang et al. - Figure 5, item 506 recites the determination of client authorization to receive access to resources, and release those resources for download to the client).

Kang et al. do not disclose, but Vaid et al. disclose an invention substantially as claimed, wherein the downloadable component is configured, in part, to determine the configuration of the client device (Vaid et al. – Column 23, lines 38-59 recite the active probing of devices on the network and providing statistics to management components, one of which being the Enterprise Policy Manager).

The motivation and obviousness arguments are the same as in Claim 3.

6. Claim 6 and 17-18, 24 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kang et al. as applied to claim 1 above, and further in view of US 5,974,549 (Golan).

As to Claim 6, Kang et al. anticipate the apparatus of claim 1, and

that is configured based on the applied dynamic policy (Kang et al. – Figure 4, item 412 recites the dynamic authentication procedure).

Kang et al. do not disclose, but Golan discloses an invention substantially as claimed, including wherein applying the restriction further comprises employing a virtual sandbox (Golan – Column 6, lines 1-5 recite the use of the virtual sandbox in a security monitoring environment).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine applying the restriction further comprises employing a virtual sandbox taught by Golan, with a policy manager, coupled to the receiver taught by Kang et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to allow a component to execute freely while enforcing compliance with security rules (Golan – Column 6, lines 1-5).

As to Claim 17, Kang et al. anticipate the method of claim 10.

Kang et al. do not disclose, but Golan discloses an invention substantially as claimed, including wherein applying the restriction further comprise configuring a virtual sandbox to intercept a communication between the client device and the resource (Golan – Column 6, lines 1-5 recite the use of the virtual sandbox in a security monitoring environment).

The motivation and obviousness arguments are the same as in Claim 6.

As to Claim 18, the combination of Kang et al. and Golan discloses an invention substantially as claimed, including the method of claim 17, wherein intercepting the communication further comprises blocking a download of at least one file to the client device (Kang et al. – Figure 5 recites blocking access to server resources).

As to Claim 24, Kang et al. anticipate the network appliance of claim 22.

Kang et al. do not disclose, but Golan discloses an invention substantially as claimed, including wherein applying the restriction further comprises employing a virtual sandbox that is configured based on the applied dynamic policy (Golan – Column 6, lines 1-5 recite the use of the virtual sandbox in a security monitoring environment).

The motivation and obviousness arguments are the same as in Claim 6.

As to Claim 29, Kang et al. anticipate the modulated data signal of claim 28.

Kang et al. do not disclose, but Golan discloses an invention substantially as claimed, including wherein applying the restriction further comprises configuring a virtual sandbox to intercept a communication between the client device and the resource (Golan – Column 6, lines 1-5 recite the use of the virtual sandbox in a security monitoring environment).

The motivation and obviousness arguments are the same as in Claim 6.

7. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kang et al. as applied to claim 10 above, and further in view of US 7,200,272 B2 (Ishikawa).

As to Claim 19, Kang et al. anticipate the method of claim 10.

Kang et al. do not disclose, but Ishikawa discloses an invention substantially as claimed, wherein applying the restriction further comprises:

if the access to the resource is terminated, performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and

enabling a disabled system command (Ishikawa – Column 5, lines 2-12 recite the client's cache manager deleting the user's cache as part of a cleanup).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command taught by Ishikawa, with applying a restriction to the access for the requested resource based on the applied dynamic policy taught by Kang et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to avoid system resources from sitting at their maximum limit, thus freeing up resources for other applications to use (Ishikawa - Column 5, lines 8-12).

8. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kang et al. as applied to claim 10 above, and further in view of US 7,107,052 B2 (Mahany).

As to Claim 20, Kang et al. anticipate the method of claim 10.

Kang et al. do not disclose, but Mahany discloses an invention substantially as claimed, including wherein applying the dynamic policy further comprises determining at least one of a connector, and an adaptor to enable the access to the resource (Mahany - Column 6, lines 47-54 recite the determination of an adaptor to provide access to resources).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine determining at least one of a connector, and an adaptor

to enable the access to the resource taught by Mahany, with applying a restriction to the access for the requested resource based on the applied dynamic policy taught by Kang et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to ensure the proper communication equipment is available.

9. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kang et al. as applied to claim 22 above, and further in view of US 6,931,546 B1 (Kouznetsov et al.).

As to Claim 26, Kang et al. anticipate the network appliance of claim 22, wherein applying the dynamic policy further comprises:

restricting access to the resource (Kang et al. - Figure 5, item 508 recites restricting access to the resource).

Kang et al. not disclose, but Kouznetsov et al. disclose an invention substantially as claimed, including if the client device is configured to restricting a download of a component (Kouznetsov et al. - Column 7, lines 16-19 recite the client restricting a download).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine if the client device is configured to restricting a download of a component taught by Kouznetsov et al., with applying a restriction to the

access for the requested resource based on the applied dynamic policy taught by Kang et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to be compatible with clients designed to detect imposter servers (Kouznetsov et al. – Column 7, lines 16-32).

10. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over the Kang et al. as applied to claim 22 above, and further in view of US 6,931,546 B1 (Kouznetsov et al.) and Non-Patent Literature on the Print Distributor 2.0 system (Print Distributor 2.0).

As to Claim 27, Kang et al. anticipate the network appliance of claim 22.

Kang et al. do not disclose, but Print Distributor 2.0 discloses an invention substantially as claimed, including intercepting a communication between the client device and the requested resource to perform at least one of preventing an access to file, and restricting an action (Print Distributor 2.0 – Pages 1-3 recite the downloadable resource called Print Distributor 2.0 which intercepts print files and restricts the launching of the print job to the printer by allowing redirection to a file).

Kang et al. do not disclose, but Kouznetsov et al. disclose an invention substantially as claimed, including if the client device is configured to restrict a download of a component (Kouznetsov et al. - Column 7, lines 16-19 recite the client restricting a download),

The motivation and obviousness arguments for Kouznetsov et al. are the same as in Claim 26.

The motivation and obviousness arguments for Print Distributor 2.0 are the same as in Claim 8.

11. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 6,954,792 B2 (Kang et al.) and further in view of US 7,337,174 B1 (Craig).

As to Claim 32, Kang et al. disclose an invention substantially as claimed, including a method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device (Kang et al. – Figure 4, item 400 recites the client sending a connection request for access to resources to a server); and

applying a dynamic policy to the access (Kang et al. – Column 13, lines 3-5 recite the client and server negotiating the authentication type, when is a dynamic process); and

applying a restriction to the access for the requested resource based on the applied dynamic policy (Kang et al. – Figure 4, item 416 recites the denial of client access to server resources).

Kang et al. do not disclose, but Craig discloses an invention substantially as claimed, including determining a level of security software enabled on the client device (Craig – Column 5, lines 1-11 recite the determination of the client's security level); and

based, in part, on the determined level of security software enabled (Craig – Column 5, lines 1-11 recite the determination of the client's security level).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine determining a level of security software enabled on the client device and based, in part, on the determined level of security software enabled taught by Craig, with applying a dynamic policy to the access taught by Kang et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to validate a user's access or verify the correct resources are present (Craig – Column 5, lines 12-16)

12. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 6,954,792 B2 (Kang et al.) and further in view of US 7,260,388 B1 (Myers).

As to Claim 33, Kang et al. disclose an invention substantially as claimed, including a method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device (Kang et al. – Figure 4, item 400 recites the client sending a connection request for access to resources to a server);

applying a restriction to the access for the requested resource (Kang et al. – Figure 4, item 416 recites the denial of client access to server resources).

Kang et al. do not disclose, but Myers discloses an invention substantially as claimed, including determining a configuration of an operating system active on the

client device (Myers - Column 5, lines 45-61 recite the determination of the client's operating system configuration); and

based on the determined configuration of the operating system (Myers - Column 5, lines 45-61 recite the determination of the client's operating system configuration).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine determining a configuration of an operating system active on the client device and based on the determined configuration of the operating system taught by Myers, with applying a restriction to the access for the requested resource taught by Kang et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to pre-qualify the resources needed (Myers – Column 5, lines 44-48).

13. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 6,954,792 B2 (Kang et al.) and further in view of US 7,328,453 B2 (Merkle, Jr. et al.).

As to Claim 34, Kang et al. disclose an invention substantially as claimed, including a method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device (Kang et al. – Figure 4, item 400 recites the client sending a connection request for access to resources to a server);

applying a restriction to the access for the requested resource (Kang et al. – Figure 4, item 416 recites the denial of client access to server resources).

Kang et al. do not disclose, but Merkle, Jr. et al. disclose an invention substantially as claimed, including determining a presence of a hacker tool active on the client device (Merkle, Jr. et al. - Column 33, lines 49-67 recite the detection of a hacker tool); and

based on the determined presence of the hacker tool (Merkle, Jr. et al. - Column 33, lines 49-67 recite the detection of a hacker tool).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine determining a presence of a hacker tool active on the client device and based on the determined presence of the hacker tool taught by Merkle, Jr. et al., with applying a restriction to the access for the requested resource taught by Kang et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to scan for threats (Merkle, Jr. et al. – Column 33, lines 49-50).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. These include

- US 7,322,004 B2 - Systems and methods for automated network policy exception detection and correction
- US 6,990,591 B1 - Method and system for remotely configuring and monitoring a communication device

- US 6,917,980 B1 - Method and apparatus for dynamic modification of internet firewalls using variably-weighted text rules
- US 6,981,257 B2 - System, method and apparatus to allow communication between CICS and non-CICS software applications
- US 7,257,623 B2 - Method and apparatus for ensuring an allowable client configuration for an application
- US 7,237,263 B1 - Remote management of properties, such as properties for establishing a virtual private network
- US 7,269,847 B2 - Firewall providing enhanced network security and user transparency
- US 6,766,407 B1 – Intelligent Streaming Framework
- US 7,313,822 B2 – Application-layer Security Method and System
- US 6,925,495 B2 – Method and System for Delivering and Monitoring an On-Demand Playlist Over a Network Using a Template
- US 6,944,761 B2 – Log-On Service Providing Credential Level Change Without Loss of Session Continuity
- US 6,684,253 B1 - Secure Segregation of Data of Two or More Domains or Trust Realms Transmitted Through a Common Data Channel
- US 7,260,224 B1 - Automated Secure Key Transfer

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Richard G. Keehn whose telephone number is 571-270-

5007. The examiner can normally be reached on Monday through Thursday, 8:30am - 7:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

RGK
/Bunjob Jaroenchonwanit/
Supervisory Patent Examiner, Art Unit 2152